IN THE CLAIMS

Please consider the claims as follows. This listing of claims will replace all prior versions and listings of claims in the application.

Claims 1-17 (Cancelled).

18. (New) A method of securing a computer system of an end user, comprising:

storing a software provider root security information object in an end user's computer system;

producing an end user root security information object based on the software provider root security information object;

receiving security information from a higher-level entity;

validating the received security information using the end user root security information object; and

updating the end user root security information object based on validated security information;

wherein the end user root security information object determines the entities the end user can trust, determines what functions a trusted entity can perform, and determines who can update the root security information object;

wherein the end user root security information object is controlled by the software provider root security information object; and

wherein the computer system refuses information from an entity that is not included in the end user root security information object.

19. (New) The method of claim 18 wherein the end user sends end user security information to the higher-level entity.

20. (New) The method of claim 19 wherein the higher-level entity sends end user security information to a software provider.

21. (New) method of claim 18 wherein the end user receives security information within a digital certificate.

22. (New) The method of claim 18 wherein the entities the end user can trust include a certification authority.

23 (New) A method of controlling a computer system, comprising:

storing a software provider root security information object in a local computing device;

producing local root security information based on the stored software provider root security information object, wherein said local root security information identifies trusted entities, provides trust information that specifies the roles that the trusted entities can fulfill, and designates who can modify the local root entity information;

receiving updated trust information;

validating the received updated trust information using the local root security information and the software provider root security information object; and

updating the local root security information with the validated trust information.

24. (New) The method of claim 23 wherein the local computing device sends local root security information to an upper-level entity.

25. (New) The method of claim 24 wherein the upper-level entity sends local root security information to a software provider.

26. (New) The method of claim 23 wherein the end user receives updated trust information embedded within a digital certificate.

27. (New) The method of claim 18 wherein the entities the local user can trust include a certification authority.

28. (New) A method of updating trust relationships of users, wherein each user includes stored software provider information and stored user root security information, the method comprising:

maintaining an upper level root security information object in a computing device, wherein the upper level root security information object includes information regarding the user root security information of each user and information on the stored software provider information; and

sending a selected user updated security information;

wherein the sent updated security information is security protected using the selected user's stored user root security information and the software provider information; and

wherein the sent updated security information includes information regarding a trusted entity.

29. (New) A method of claim 28 wherein the sent updated security information regards a certification authority.

30. (New) A method of claim 28 wherein the sent updated security information is embedded in a digital certificate.

31. (New) A method of claim 30 wherein the digital certificate is in accord with X.509 version 3.

32. (New) A method of claim 28 wherein the sent updated security information is also sent to a software provider.